IEEE Internet of Things Journal Special Issue on
"*Secure Embedded IoT Devices for Resilient Critical Infrastructures*"

The Internet of Things (IoT) opens the door to new technological opportunities for a wide range of applications that cover e-health, smart homes and automation, e-commerce, location-based services, smart vehicles, fleet management and remote system monitoring. However, at the same time as these technological opportunities grow so does the threat surface for potential adversaries targeting at various, interconnected ICT systems and consequently at ICT-dependent critical systems, such as SCADA (Supervisory Control and Data Acquisition Systems) systems. At this point, attackers could take advantage from the incorporation of the paradigm to exploit new security gaps, probably caused by unforeseen interoperability and adaptability problems.

Indeed, the deployment of Internet-enabled embedded devices that are distributed over major critical domains, may create indirect and non-obvious inter-connections with the underlying Critical Infrastructures (CIs). Examples of such inter-connected systems may include traffic monitoring and control systems communicating with smart vehicles, energy related systems communicating with smart homes and smart meters, monitoring systems connected with autonomous sensors in nuclear plants, power grids and body area networks. There is a need to further explore the security issues related to IoT technologies to assure the resilience of CIs against advanced IoT-based attacks. The goal of this special issue is therefore to address the diverse security challenges and related to IoT-enabled CIs (IoT-CIs) and their resilience to advanced threats.

Suggested topics include, but are not limited to, the following:

- Security analysis and requirements in the coupling of IoT-CIs
- Vulnerabilities, threat models and risk management in IoT-CIs
- Reference architectures for the secure coupling of IoT in CI scenarios
- Embedded security for mobile devices and BYOD
- Network-layer attacks and defense mechanisms between IoT devices and CIs
- Key management and access control in IoT-CIs
- Resilience models for advanced threats in IoT-CIs
- Advanced and lightweight awareness models for large IoT-CIs
- Privacy and location privacy for IoT-CIs

Important dates:

Submissions Deadline: October 1, 2018	First Reviews Due: December 15, 2018
Revision Due: January 15, 2019	Second Reviews Due/Notification: Feb. 15, 2019
Final Manuscript Due: March 15, 2019	Publication Date: 2019

Submission Guidelines:

All original manuscripts or revisions to the IEEE IoT Journal must be submitted electronically through IEEE Manuscript Central, http://mc.manuscriptcentral.com/iot. Solicited original submissions must not be currently under consideration for publication in other venues. Author guidelines and submission information can be found at http://iot.ieee.org/journal.

Guest Editors:

- *Cristina Alcaraz*, University of Malaga, Spain alcaraz@lcc.uma.es
- *Mike Burmester*, Florida State University, USA burmester@cs.fsu.edu
- *Jorge Cuellar,* Siemens, Germany, jorge.cuellar@siemens.com
- *Xinyi Huang,* Fujian Normal University, China, xyhuang81@gmail.com
- *Panayiotis Kotzanikolaou,* University of Piraeus, Greece, pkotzani@unipi.gr
- *Mihalis Psarakis,* University of Piraeus, Greece, mpsarak@unipi.gr